In the claims:

1. (Currently amended) ~~In a design zone system with~~ A method for providing a

secure access of a partner to the development environment of an owner comprising

the steps of : ~~means for~~ starting a VPN tunnel between workstations to establish a

secure encrypted tunnel end to end wherein each partner is identified with a different

VPN group/password; ~~means for~~ starting a session by the partner in a Web page on a

portal machine that authenticates ~~thru~~ through LDAP (Lightweight Directory Access

Protocol) ~~the user/password~~ a user identification and password of ~~the person~~ user;

~~means for~~ routing the session to an engagement box depending on the ~~person~~ user

where the engagement boxes each include a server with an operating system and are

on network segments separated by firewall boxes with another logon/password and is

validated ~~thru~~ through second LDAP and wherein all users of the same partner are all

launching on the same engagement box; ~~and means for~~ accessing data and

applications from ~~that~~ an engagement box on Network File system storage

authenticated second LDAP to a design zone common resource of said owner with

~~get benefit of~~ a big compute farm composed of many high-end servers in a ~~very~~

secure way, submitting batch or interactive jobs to said design zone ; and ~~a method of~~

providing for each application host in said design zone a highly secure access to EDA

licenses from license servers with dynamically changing access ports of ~~an~~ said

owner inside an Intranet of said owner without opening all such access ports for all

hosts and creating a security risk comprising the steps of:

    providing a license proxy server in said design zone that dynamically determines

    the addresses of the changing access ports of the license servers in said Intranet;

    and

said application hosts inside said design zone contacting the license proxy server which in turn fetches the appropriate EDA licenses from said license servers in said Intranet of said owner.

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Canceled)

8. (Canceled)

9. (Canceled)

10. (Canceled)

11. (New)   A method to provide secure access by application hosts in a design zone to EDA licenses managed by software daemon manager running FLEXLM on license servers behind a firewall inside an Intranet of an owner without opening all inbound ports greater than 1023 from all the hosts in the design zone on which EDA applications are run, where FLEXLM has a manager daemon and a vendor daemon and said vendor daemon has a random changing port number above 1023 for access and said manager daemon listens on a known TCP port that is greater than 1023 and when an application host makes a connection to this known port FLEXLM replies back with the port on which the vendor daemon is listening, comprising the steps of:

providing a license proxy server inside the design zone that listens on the FLEXLM manager port;

intercepting EDA license requests by the application host by said proxy server and said proxy server initiating a connection to said manager daemon of said license server on behalf of the application host and FLEXLM responding with port number of the vendor daemon in a reply packet;

said proxy server intercepting this packet and reading the port number and creating another listening socket on the same port as the vendor port, and

said application host initiating a connection to the vendor port on the proxy server which in turn initiates a connection to the vendor port on the license server and relays the packets back and forth between the application hosts and the appropriate license server.

12. (New) A system for providing a secure access of one or more partners to the development environment of an owner comprising:

means for starting a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

means for starting a session by the partner in a Web page on a portal machine that authenticates through LDAP (Lightweight Directory Access Protocol) a user identification and password of a user;

means for routing the session to an engagement box depending on the a user where the engagement boxes each include a server with an operating system and are on network segments separated by firewall boxes with another logon/password and is validated through second LDAP and wherein all users of the same partner are all launching on the same engagement box;

means for accessing data and applications from an engagement box on Network File system storage authenticated second LDAP to a design zone common resource of said owner with a big compute farm composed of many high-end servers in a secure way;

means for submitting batch or interactive jobs to said design zone; and

means for providing for each application host in said design zone a highly secure access to EDA licenses from license servers with dynamically changing access ports of said owner inside an Intranet of said owner without opening all such access ports for all hosts and creating security risk comprising:

a license proxy server in said design zone that determines the dynamically changing access ports of the license servers in said Intranet; and

said application hosts inside said design zone contacting the license proxy server which in turn fetches the appropriate EDA licenses from said license servers in said Intranet of said owner.

13. (New)   A method for providing a secure access of one or more partners to the development environment of an owner comprising the steps of :

starting a VPN tunnel between workstations to establish a secure encrypted tunnel end to end wherein each partner is identified with a different VPN group/password;

starting a session by the partner in a Web page on a portal machine that authenticates through LDAP (Lightweight Directory Access Protocol) a user identification and password of a user;

routing the session to an engagement box depending on the user where the engagement boxes each include a server with an operating system and are on network segments separated by firewall boxes with another logon/password and is validated

through second LDAP and wherein all users of the same partner are all launching on the same engagement box;

accessing data and applications from an engagement box on Network File system storage authenticated second LDAP to a design zone common resource of said owner with a big compute farm composed of many high-end servers in a secure way; submitting batch or interactive jobs to said design zone; and providing for each application hosts in said design zone a highly secure access to EDA licenses from FLEXLM controlled servers of said owner inside an Intranet of said owner without a security risk of opening all ports greater than 1023 for all hosts in the design zone, where FLEXLM has a manager daemon and a vendor daemon and said vendor daemon has a random changing port number above 1023 for access and said manager daemon listens on a known TCP port that is greater than 1023 and when an application host makes a connection to this known port FLEXLM replies back with the port on which the vendor daemon is, comprising the steps of:

providing a license proxy server inside the design zone that listens on the FLEXLM manager port and intercepts EDA license requests by the application host and initiates a connection to a manager daemon of said license server on behalf of the application host, said license manager responding with port number of the vendor daemon in a reply packet;

said proxy server intercepting said reply packet and reading the port number and creating another listening socket on the same port as the vendor port, and said application host initiating a connection to the vendor port on the proxy server and said proxy server

initiating a connection to the vendor port on the license server and relays the packets back

and forth between the application hosts and the appropriate license server.

14. (New)   A system for providing a secure access of one or more partners to the

development environment of an owner comprising:

means for starting a VPN tunnel between workstations to establish a secure

encrypted tunnel end to end wherein each partner is identified with a different VPN

group/password;

means for starting a session by the partner in a Web page on a portal machine

that authenticates through LDAP (Lightweight Directory Access Protocol) a user

identification and password of a user;

means for routing the session to an engagement box depending on the a user

where the engagement boxes each include a server with an operating system and are on

network segments separated by firewall boxes with another logon/password and is

validated through second LDAP and wherein all users of the same partner are all

launching on the same engagement box;

means for accessing data and applications from   an engagement box on Network

File system storage authenticated second LDAP to a design zone common resource of

said owner with a big compute farm composed of many high-end servers in a secure way;

means for submitting batch or interactive jobs to said design zone; and

means for providing for each application hosts in said design zone a highly secure

access to EDA licenses from FLEXLM controlled servers of said owner inside an

Intranet of said owner without a security risk of opening all ports greater than 1023

for all hosts in the design zone, where FLEXLM has a manager daemon and a vendor

daemon and said vendor daemon has a random changing port number above 1023 for

access and said manager daemon listens on a known TCP port that is greater than

1023 and when an application host makes a connection to this known port FLEXLM

replies back with the port on which the vendor daemon is, comprising:

a license proxy server inside the design zone that listens on the FLEXLM manager port

and intercepts EDA license requests by the application host and initiates a connection to a

manager daemon of said license server on behalf of the application host,

said license manager daemon responding with port number of the vendor daemon in a

reply packet;

said proxy server intercepting said reply packet and reading the port number and creating

another listening socket on the same port as the vendor port, and said application host

initiating a connection to the vendor port on the proxy server and said proxy server

initiating a connection to the vendor port on the license server and relays the packets back

and forth between the application hosts and the appropriate license server.